NATIONAL INFRASTRUCTURE PROTECTION CENTER

HIGHLIGHTS

A publication providing information on infrastructure protection issues, with emphasis on computer and network security matters.

Issue 7-01
July 15, 2001

Editors: Linda Garrison
Martin Grand

- **Network Defense: The Legal Aspects of Retaliation**
- **Interdependencies: Blackouts Present Challenges to Emergency Services**
- **Information Sharing and Analysis Center-Electric Power Sector (ISAC-EPS)**
- **Web Vulnerabilities: Unicode-related Flaw Continues to Be Exploited**

For more information, or to be added to the distribution list, please contact the NIPC Watch at nipc.watch@fbi.gov or call (202) 323-3204.

We welcome your comments and suggestions for improving this product. To provide comments, contact the Editors at (202) 324-0334 or (202) 324-0353.

This issue has an overall classification of AUnclassified." This publication may be disseminated further without express permission.

Network Defense: The Legal Aspects of Retaliation

Retaliating against the apparent source of an intrusion or attack may have a greater chance of landing the original victim in court than it has of punishing the perpetrator.

Legal Issues

A number of state and federal laws prohibit unauthorized intrusion and malicious attacks against computer networks. These include but are not limited to:

- **18 U.S.C. § 1029** Fraud and related activity in connection with access devices which can include the unauthorized use of a password to intrude into an enterprise network;

- **18 U.S.C. § 1030** Fraud and Related Activity in Connection with Computers section (5)(A): "[whoever] knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer", which may be applied to the malicious introduction of a virus into, or a denial-of-service attack against, a sector member's computer networks.

- Multiple state laws, such as: **Massachusetts General Law Chapter 266 Section 120F** Unauthorized access to computer system: "Whoever, without authorization, knowingly accesses a computer system by any means … and fails to terminate such access, shall be punished by imprisonment in the house of correction for not more than thirty days or by a fine of not more than one thousand dollars, or both."

Retaliatory Strike Issues

A counterattack against a system believed to be the source of an attack may violate state and/or federal laws pertaining to unauthorized access or disruption of computers and computer networks. Furthermore, one can never be certain that the apparent source of a network intrusion or disruption is in fact the *actual* source. Rather than launching a countermeasure against an innocent bystander, a more prudent action would be to contact the proper authorities, including one's local FBI Field Office. (For more information on incident reporting procedures, see http://www.nipc.gov/incident/incident.htm).

Sector Member Policy Issues

Critical Infrastructure sector members are strongly advised to have a computer network defense policy in place. Employees charged with the protection of an enterprise network should be educated as to the recommended steps to take in the event of a network intrusion or denial-of-service attack. To reduce the victim's liabilities following an intrusion or attack, the company's remedial policy should specify a "no counterattack" rule with clear instructions on how to contact the appropriate law enforcement agency.

Interdependencies: Blackouts Present Challenges to Emergency Services

Contingency plans and coordination are essential in preparing for possible electrical outages that can place a strain on emergency service providers.

Plans Are a Part of Business

Electric companies have plans in place for dealing with temporary outages caused by accidents, severe weather, or other incidents. Service priorities are usually reserved for hospitals, police, fire, rescue services, customers on life support, etc., and considerable effort is made to keep the list of priority customers short. The list of priorities typically is proposed by the electric company and approved by a state regulatory body, usually a public utility commission (PUC). Obtaining a priority usually means that service to a particular customer will be among the last to be curtailed (in a controlled outage) and among the first to be restored; it does not mean service is guaranteed.

Operations May Be Complicated

Existing electric company emergency plans are typically less able to cope with longer term or continuing emergencies, such as the inability of available electricity generation to meet expected demand over coming months or years. Over that kind of time frame, cross-sector interdependencies may become more problematic.

For example, repeated loss of electricity, especially in large urban areas, may seriously affect law enforcement services. In some cases, prior knowledge of intended patterns of rolling blackouts may even raise the likelihood of events such as civil disobedience, looting, loss of life, and property damage. The ability of law enforcement units to respond to these events could be reduced as a result of traffic congestion from inoperative traffic signals and gasoline pumps.

Where the curtailment of electric service is limited to certain sections of a city, large numbers of people could be moving to community shelters if their environmental systems are unable to operate at acceptable levels. Other emergency responders and health care providers would face similar challenges.

Mitigation

Customers who believe that priority electric service is warranted for their facilities should notify their service provider and their PUC. Self-help initiatives are also recommended and can take the form of installing dual-feed service (from a separate feeder line or a transmission line if one is conveniently available) or of installing distributed generation or cogeneration.

Emergency service providers should acquaint themselves in advance, not only with the identity and location of electricity customers with true service priorities but also with emergency supply plans for facilities with cross-sector importance. This planning should

include facilities whose continuous operation is considered critical to the basic needs of society but which may not necessarily be registered on any electric service priority list.

Information Sharing and Analysis Center-Electric Power Sector (ISAC-EPS)

This is the first in a series of articles regarding the current status of ISACs established under Presidential Decision Directive 63 (PDD-63).

Background

In September 1998, the North American Electric Reliability Council (NERC) was asked by the Secretary of Energy to assume Sector Coordinator responsibilities for the electric power sector (as defined in PDD-63). In fall 2000, NERC was formally recognized as the Information Sharing and Analysis Center - Electric Power Sector (ISAC-EPS).

NERC Membership

NERC is a not-for-profit corporation comprised of ten Regional Councils. Council members come from all segments of the power industry: investor-owned utilities, federal power agencies, rural electric cooperatives, state, municipal and provincial utilities, independent power producers, and power marketers. These entities account for virtually all the electricity supplied in the United States, Canada, and a portion of Baja California Norte, Mexico.

Status of NERC's ISAC Activities

NERC and the NIPC have worked closely to establish a *voluntary* Indications, Analysis and Warning (IAW) Program. The IAW Program is built on a trusted partner basis and features timely reporting of incidents to NIPC that meet one or more of 15 pre-established thresholds and criteria. This program has been established to enable the NIPC to provide timely, accurate, and actionable warning for both operational and cyber threats or attacks on the national electric power infrastructure.

The IAW Program is now being rolled out nationally. In its support of the ISAC, the NIPC has presented classified threat briefings, sponsored ISAC staff for security clearances, and provided secure communications equipment. The ISAC staff is available on a 24/7 basis to handle sector incident reports and disseminate NIPC warning products.

Programmatic Details

The IAW Program is defined by a set of Standard Operating Procedures (SOP) that are a shared responsibility of NERC and the NIPC. The fact that the interconnected power grid makes no distinction regarding our national border with Canada means the IAW program must be well coordinated between the FBI and the Canadian government.

Additional Information

For more information on the ISAC-EPS, please see related materials on the NERC website at **http://www.nerc.com/~filez/cip.html**, or contact Lou Leffler at lou.leffler@nerc.com or (609) 452-8060. Alternatively, Harvey Blumenthal may be contacted at the NIPC at (202) 324-0339 or by e-mail at hblumenthal.nipc@fbi.gov.

Web Vulnerabilities: Unicode-related Flaw Continues to Be Exploited

A Web server exploit related to Unicode continues to grab headlines despite the fact that a software fix for the vulnerability has been available since August 2000.

Discovered last year, a security vulnerability in Microsoft's popular Internet Information Server (IIS) Web server relating to implementation of Unicode continues to attract the attention of malicious actors on the Internet. Although this bug is relatively old in the fast-paced world of security analysis, its exploitation continues to make headlines. Various exploits have been developed to take advantage of this vulnerability, and many recent Internet intrusions have reportedly been performed using different versions of it.

Unicode: Encoding the World's Languages

Unicode provides a unique representation for tens of thousands of characters used by the world's writing systems. Implementation of Unicode has become a significant software trend met with wide acceptance; the Unicode Standard has been adopted by many of the leaders of the software industry.

Security Implications of Unicode

However, last year security experts noted that widespread implementation of Unicode could have serious security implications. One of these issues arises from the fact that under Unicode, a single character may have multiple representations. For example, the exploit against IIS utilizes a variation of the common so-called 'dot dot' directory traversal attack. In this type of attack, the string '/..' is included in a request to a server in order to allow an attacker to access files outside of the server's Web root directory. Most Web servers can recognize this type of attack and strip any extra slashes and dots from the request. The IIS exploit, however, works by substituting Unicode codings in place of the usual characters; in this case, the server will not recognize the malicious pattern and allow the attack to succeed. According to Microsoft Security Bulletin MS00-078, this vulnerability can enable a malicious user to execute arbitrary code on an affected server. This bulletin and the accompanying software patch may be found on the company's Web site at http://www.microsoft.com/technet/security/bulletin/ms00-078.asp.

The continued popularity of the IIS Unicode exploit is evidenced by the fact that the recently discovered sadmind/IIS worm exploits this vulnerability as one part of its automated attack on Internet-connected hosts. (For more information on this worm, see the CERT Coordination Center's advisory at **http://www.cert.org/advisories/CA-2001-11.html**.)

Future Challenges

Many predictions have been made concerning the challenges of future Unicode vulnerabilities. The Unicode Consortium has taken steps to address some of these issues, and software companies are developing products with safer implementations of this standard. No matter what future vulnerabilities are brought to light, however, this case study illustrates that awareness and keeping up with vendor-supplied security patches is the best defense against current and future attacks.